Getting started

Symantec AntiVirus™ for Blue Coat™ Security

Copyright © 2003 Symantec Corporation.
All rights reserved.
Printed in the U.S.A.
10/03 10199300
Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Symantec AntiVirus is a trademark of Symantec Corporation. Blue Coat is a trademark of Blue Coat Systems, Inc., in the United States and other countries. Other brands and products are trademarks of their respective holder/s.

About Symantec AntiVirus for Blue Coat Security

Symantec AntiVirus™ version 4.3 for Blue Coat™ Security provides integrated virus scanning and repair capabilities for the line of Blue Coat Security appliances that support the Internet Content Adaptation Protocol (ICAP). Symantec AntiVirus for Blue Coat Security features the Symantec AntiVirus Scan Engine, a carrier-class virus scanning and repair engine, which protects your network from Web traffic that contains viruses. The Symantec AntiVirus Scan Engine features all of the virus-scanning technologies that are available in Symantec AntiVirus products, which makes the Symantec AntiVirus Scan Engine one of the most effective virus solutions available for detecting and preventing virus attacks.

The Blue Coat Security appliance is a caching proxy server that handles all of the HTTP traffic on your network. As the Blue Coat Security appliance retrieves requested information from the Web, it also caches (stores a copy on disk) the information and, where possible, serves multiple requests for the same Web content from the cache. Blue Coat Security clients use ICAP to communicate with the Symantec AntiVirus Scan Engine to request virus scanning as a file is retrieved from the Web, before it is sent to the requesting user. When a virus is found in a downloaded file and the file is repaired, the clean file is cached and forwarded to the requesting user. When a virus is found that cannot be repaired, access to the infected file is denied.

What's new in version 4.3

Symantec AntiVirus for Blue Coat Security version 4.3 includes the following new features:

- POST transaction antivirus scanning: Symantec AntiVirus for Blue Coat Security now scans files that are being posted to the Internet. The antivirus scanning and logging policies that are configured on the scan engine now apply to POST transactions as well.
- Upgrade installation support: You now can install an upgrade to Symantec AntiVirus for Blue Coat Security over an existing installation (without first uninstalling the previous version). Any configuration changes and customizations that have been made are preserved during the upgrade.

- Upgraded logging features: Logging for each logging destination is activated individually by selecting a desired logging level for that destination. Selecting the logging level lets you choose the types of events for which log messages are generated. You can select a different logging level for each logging destination.
- Dynamic thread pool for antivirus scanning: The pool of scanning threads that is available to the Symantec Antivirus Scan Engine for antivirus scanning now dynamically adjusts to the load that is being processed.
- Command-line scanner: The Symantec AntiVirus Scan Engine now includes a command-line scanner, which lets you send files to be scanned for viruses via the command line. You can repair infected files and delete those that are unrepairable.

The Symantec AntiVirus Scan Engine also includes a user comforting feature, called data trickle. This feature prevents a user who downloads a large file from the Internet from receiving a session time-out error by trickling small amounts of the file to the user while the file is being scanned. Blue Coat Security also provides its own user comforting feature (the patience page setting). To prevent redundancy, Symantec recommends that you use the patience page setting on the Blue Coat Security appliance to provide user comforting.

About ICAP

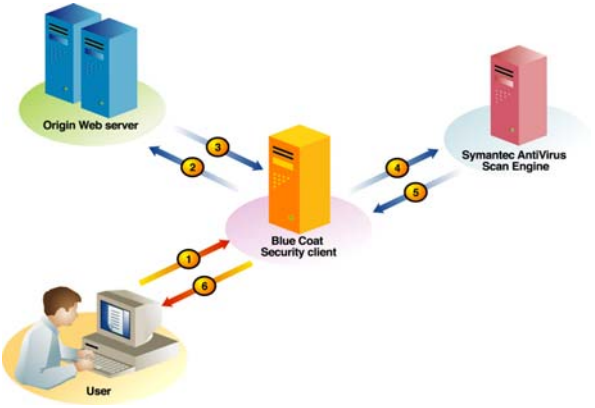
Blue Coat Security clients use ICAP to communicate with the Symantec AntiVirus Scan Engine to request virus scanning. ICAP is a lightweight protocol for executing a remote procedure call on HTTP messages. ICAP is part of an evolving architecture that lets corporations, carriers, and ISPs dynamically scan, change, and augment Web content as it flows through ICAP servers. The protocol lets ICAP clients pass HTTP messages to ICAP servers for some sort of adaptation (transformation or other processing, such as virus scanning). The server executes its adaptation service on messages and responds to the client, usually with modified messages. The adapted messages might be either HTTP requests or HTTP responses.

How the Symantec AntiVirus Scan Engine works with the Blue Coat Security client

You can use a single Symantec AntiVirus Scan Engine to support a Blue Coat Security client, or you can use multiple scan engines to handle larger scan volumes. To use multiple scan engines, you must create an ICAP service cluster on the Blue Coat Security appliance, which lets load balancing be handled automatically through the cluster configuration.

A typical integration of the Symantec AntiVirus Scan Engine with a Blue Coat Security client is shown in Figure 1-1.

Figure 1-1 Integration of the Symantec AntiVirus Scan Engine with the Blue Coat Security client



1. A user sends a request to the origin server through the Blue Coat Security client.
2. The Blue Coat Security client checks the cache, and not finding the requested page, forwards the request to the origin server.
3. The origin server returns the page to the Blue Coat Security client.
4. The Blue Coat Security client sends the file to the Symantec AntiVirus Scan Engine.
5. The Symantec AntiVirus Scan Engine scans the file, repairs the infection, and returns a clean file to the Blue Coat Security client.
6. The Blue Coat Security client caches the page and returns it to the user.

Scanning files for viruses

When the Symantec AntiVirus Scan Engine is contacted by the Blue Coat Security client to scan a file, a small amount of file data is transferred to the Symantec AntiVirus Scan Engine. This data contains the first 4 bytes of the file to be scanned. The Symantec AntiVirus Scan Engine examines this data to determine whether to scan the file. If the file extension is one that should be scanned, the Symantec AntiVirus Scan Engine requests the remainder of the file from the Blue Coat Security client and scans it.

If the file is a container file and contains embedded files, the Symantec AntiVirus Scan Engine extracts the embedded files from the container file and scans the files with extensions that match those that are specified for scanning. When scanning is complete, the container file is reassembled. Infected files that are embedded in the container file can be repaired or deleted, depending on how the scan engine is configured to handle infected files.

Handling of infected files

When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following:

- Scan only: Deny access to the infected file, but do nothing to the infected file.
- Scan and delete: Delete all infected files without attempting repair.
- Scan and repair files: Attempt to repair infected files and deny access to unrepairable files (but do not delete files that cannot be repaired from archive files).
- Scan and repair or delete: Attempt to repair infected files, and delete any unrepairable files from archive files.

Alerting users when infected files cannot be repaired

The Symantec AntiVirus Scan Engine supplies an HTML text message to display when a requested file is blocked. (Access to a file is blocked by the Blue Coat Security client when the file contains a virus that cannot be repaired.) The default HTML text file indicates that access is denied because the file contains a virus. The text that is displayed can be customized by editing the file or substituting an alternate file.

See "Changing the ICAP access denied message" on page 7.

Preparing for installation

To interface with the Symantec AntiVirus Scan Engine, the Blue Coat Security appliance must be ICAP-enabled for ICAP version 1.0, as presented in RFC 3507 (April 2003). Blue Coat Security appliances that are running SG2.1.06 or later meet this requirement. The Symantec AntiVirus Scan Engine cannot be installed on the Blue Coat Security appliance. The scan engine must be installed on another computer on the network. Ensure that the computer on which you plan to install the Symantec AntiVirus Scan Engine meets the system requirements that are listed in the *Symantec AntiVirus Scan Engine Implementation Guide*.

After you have installed the Symantec AntiVirus Scan Engine, you must configure both the scan engine and the Blue Coat Security appliance.

Configuring the Symantec AntiVirus Scan Engine to use ICAP

The Symantec AntiVirus Scan Engine must be configured to use ICAP as the communication protocol. At installation, ICAP is the default communication protocol. If the scan engine is already installed and using a different protocol, you can change the protocol through the administrative interface. Once you have selected ICAP, you must configure several ICAP-specific options.

If you are installing the Symantec AntiVirus Scan Engine, see "Selecting ICAP at installation" on page 3.

If the Symantec AntiVirus Scan Engine is already installed and another protocol is in use, see "Configuring ICAP-specific options on the scan engine" on page 3.

Selecting ICAP at installation

When you install Symantec AntiVirus for Blue Coat Security, ICAP is the default protocol type. The default port number is 1344.

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Configuring ICAP-specific options on the scan engine

After you install the Symantec AntiVirus Scan Engine, you can configure several settings that are specific to the ICAP protocol. If the Symantec AntiVirus Scan Engine has already been configured to use another protocol, you can change the protocol to ICAP via the administrative interface. For more information about accessing the administrative interface, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

The protocol-specific options for ICAP are described in Table 1-1.

Table 1-1 Protocol-specific options for ICAP

Option	Description
Scan engine bind address	By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address.
Port number	The port number must be exclusive to the Symantec AntiVirus Scan Engine. For ICAP, the default port number is 1344. If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. If you are installing more than one instance of the Symantec AntiVirus Scan Engine on a single computer, each scan engine service must have a unique port number.
HTML message displayed for infected files	The Symantec AntiVirus Scan Engine includes a default HTML message to display to users when access to a file is denied because it contains a virus. You can customize this message by specifying an alternate path and file name or by editing the existing file. If you edit the existing file, you do not have to change this setting. See "Changing the ICAP access denied message" on page 7.
ICAP scan policy	When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following: ■ Scan only: Deny access to the infected file, but do nothing to the infected file. ■ Scan and delete: Delete all infected files without attempting repair. ■ Scan and repair files: Attempt to repair infected files and deny access to unrepairable files (but do not delete files that cannot be repaired from archive files). ■ Scan and repair or delete: Attempt to repair infected files, and delete any unrepairable files from archive files.
Data trickle	When a user attempts to download an extremely large or complex file from the Internet, antivirus scanning can cause a delay during which the requesting browser (and thus the user) receives no feedback on the progress of the download. You can use the data trickle feature to provide users with a quicker download response and avoid potential session time-out errors. When data trickle is enabled, the requested file is sent (trickled) to the user in small amounts at regular intervals until the scan is complete. **Note:** To prevent redundancy, Symantec recommends that you use the Blue Coat Security patience page feature and not activate data trickle. Data trickle is disabled by default on the Symantec AntiVirus Scan Engine. For more information about Blue Coat Security's patience page feature, see the appropriate Blue Coat Security documentation.

To configure ICAP-specific options on the scan engine

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **ICAP**.
   The configuration settings display for the selected protocol.
3. In the Scan Engine bind address box, type a bind address, if necessary.
   By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address.
4. In the Port number box, type the TCP/IP port number to be used by the Blue Coat Security client to pass files to the Symantec AntiVirus Scan Engine for scanning.
   The default setting for ICAP is port 1344.
5. In the HTML message displayed for infected files box, type the path and file name to supply an alternate HTML file, if necessary.
6. In the ICAP scan policy list, select how you want the Symantec AntiVirus Scan Engine to handle infected files.
   The default setting is Scan and repair or delete.

7 Verify that the Enable Trickle box is not checked.
Data trickling is disabled by default.
For more information about how data trickle works, warnings, and limitations, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

8 Click **Confirm Changes** to save the configuration.

9 Do one of the following:
- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration. If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

Controlling which file types are scanned

To specify the types of files to be scanned for viruses, you must configure settings on both the Blue Coat Security client and the Symantec AntiVirus Scan Engine.

The Blue Coat Security client makes an initial determination, based on MIME type or file extension, about whether to pass a file to the Symantec AntiVirus Scan Engine for scanning. You configure which files are passed to the Symantec AntiVirus Scan Engine for scanning when you set up the Web Content Policy for virus scanning on the Blue Coat Security client. The recommended setting is to configure the Blue Coat Security client to pass all files to the Symantec AntiVirus Scan Engine for virus scanning.

See "Creating Web Content and Web Access Policies for virus scanning" on page 9.

The Symantec AntiVirus Scan Engine also must be configured to scan selected file types. The scan policy on the Symantec AntiVirus Scan Engine is equally as important as the Blue Coat Security policy because it is used after the scan engine receives a file from the Blue Coat Security client to determine which files to scan of those that are contained in archive or container file formats. The recommended setting is to configure the scan engine to scan all files except those with extensions that are in a prepopulated exclusion list.

All top-level files that are sent by the Blue Coat Security client to the Symantec AntiVirus Scan Engine are scanned regardless of file extension. The scan policy on the Symantec AntiVirus Scan Engine is used to determine which files to scan of those that are contained in archive or container file formats. You can control which embedded files are scanned by specifying (on the Symantec AntiVirus Scan Engine) the extensions that you do not want to scan (using an exclusion list) or by specifying extensions that you want to scan (using an inclusion list), or you can scan all file types regardless of extension.

Note: Inclusion and exclusion lists by definition do not scan all file types; therefore, new types of viruses might not always be detected. Scanning all files regardless of extension is the most secure setting, but it imposes the heaviest demand on resources. During virus outbreaks, you might want to scan all files even if you normally control the file types that are scanned with the inclusion or exclusion list.

The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions that are listed in a prepopulated exclusion list. This is the recommended setting for Symantec AntiVirus for Blue Coat Security. The default exclusion list contains file types that are unlikely to contain viruses, but you can edit this list.

Using an inclusion list to control which types of files are scanned is the least secure setting. Only those files types that are listed in an inclusion list are scanned; therefore, with an inclusion list, there is an almost limitless number of possible file extensions that are not scanned. For this reason, the inclusion list is not prepopulated, but you can populate this list if you want to limit the file types that are scanned.

Specify which file types to scan

You can scan all files regardless of extension on the Symantec AntiVirus Scan Engine, or you can control which file types are scanned by specifying extensions that you do not want to scan or that you want to scan.

To scan all files regardless of extension

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, click **Scan all files regardless of extension**.

3 Click **Confirm Changes** to save the configuration.

4 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration. If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

To scan all files except for those with extensions that are in the exclusion list

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, click **Scan all files except those with the following extensions**.

3 Edit the extension list to add extensions that you do not want to scan or delete extensions that you want to scan.

Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To exclude files with no extension, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.

4 To restore the default extension list, click **Restore default lists**.

5 Click **Confirm Changes** to save the configuration.

6 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration. If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

To scan only files with extensions that are in the inclusion list

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, check **Scan files with the following extensions**.

3 Edit the extension list to add extensions that you want to scan or delete extensions that you do not want to scan.

Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To scan files that have no extensions, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.

4 Click **Confirm Changes** to save the configuration.

5 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration. If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

Selecting the maximum number of threads available for scanning

The pool of scanning threads that is available to the Symantec AntiVirus Scan Engine for antivirus scanning dynamically adjusts to the load that is being processed. You can change a number of parameters to control the dynamic thread pool. You can select the maximum number of threads that are available for scanning through the scan engine administrative interface. Additional parameters can be adjusted by editing the scan engine configuration file in accordance with the Symantec AntiVirus Scan Engine documentation.

The default setting for the maximum number of scanning threads on the Symantec AntiVirus Scan Engine is 128. When you select the maximum number of scanning threads that are available on the scan engine, consider the maximum number of connections that you select in configuring the individual scan engine as an ICAP service for the Blue Coat Security appliance. The maximum

number of scanning threads on both should be the same or very close.

To select the maximum number of threads available for scanning

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. In the Maximum number of threads allowed for scanning box, type the maximum number of threads that are allowed for concurrent scanning.
   The default number of threads is 128. Do not configure more than 256 threads.
3. Click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration. If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

Changing the ICAP access denied message

Access to a file is blocked by the Blue Coat Security appliance when the file contains a virus that cannot be repaired. The Symantec AntiVirus Scan Engine supplies an HTML text message to the Blue Coat Security appliance to display to the user when a requested file is blocked. The default text indicates that access is denied because the file contained a virus.

The ICAP access denied HTML file is installed automatically during the Symantec AntiVirus Scan Engine installation. For Solaris and Linux, the default location and file name of the HTML file is /opt/SYMCScan/etc/symcsinf.htm. For Windows 2000 Server/Advanced Server, the default location and file name of the file is C:\Program Files\Symantec\Scan Engine \SYMCSINF.htm.

The default text that is in the ICAP access denied message is as follows:

The page or file you just requested had a virus and was blocked by the Symantec AntiVirus Scan Engine.

You can customize the text that is displayed in one of the following ways:

- Specify an alternate HTML file.
  See "Configuring ICAP-specific options on the scan engine" on page 3.
- Edit the ICAP access denied HTML file.

To change the ICAP access denied message

1. Locate the Symantec AntiVirus Scan Engine ICAP access denied HTML file and open it with a text editor.
2. Make your changes to the file.
3. Save the file.
4. Stop and restart the Symantec AntiVirus Scan Engine.

Integrating virus scanning on the Blue Coat Security appliance

To interface with Symantec AntiVirus for Blue Coat Security, the Blue Coat Security appliance must be ICAP-enabled for ICAP version 1.0 and must be running SG2.1.06 or later. The Blue Coat Security client should be configured in accordance with the appropriate Blue Coat documentation and should be functioning properly before integrating virus scanning.

To integrate virus scanning on the Blue Coat Security appliance, do the following (via the Blue Coat Management Console or in command-line mode):

- Create new ICAP services for incoming and outgoing HTTP traffic for each Symantec AntiVirus Scan Engine.
  If you are using multiple Symantec AntiVirus Scan Engines, repeat this step for each scan engine.
- Create a separate ICAP cluster for incoming and outgoing traffic and add the appropriate scan engine ICAP services to the cluster.

  Note: This step is only applicable if you plan to use multiple scan engines to support virus scanning.

- Create a Web Content Policy (for incoming HTTP traffic) and a Web Access Policy (outgoing HTTP traffic) for virus scanning and configure the scan engine ICAP service or cluster as the virus scanner.

Creating an ICAP service for the scan engine

You must create and configure an ICAP service for both incoming and outgoing traffic for each Symantec AntiVirus Scan Engine. If you are using multiple Symantec AntiVirus Scan Engines to support virus scanning, you must do the same for each scan engine.

For more information, see the Blue Coat Security appliance documentation.

Table 1-2 shows the recommended settings for configuring the ICAP service on the Blue Coat Security client.

Table 1-2 Recommended settings for configuring the scan engine as an ICAP service

Management Console setting	Recommended value
ICAP version	1.0
Service URL	For incoming HTTP traffic, use: icap://<scanengineservername>/avscanresp For outgoing HTTP traffic (POST transactions), use: icap://<scanengineservername>/avscanreq
Vendor for ICAP service	Symantec You must select Symantec to ensure proper functionality.
Maximum number of connections	128 The maximum number that should be used for this setting is 256 scan threads. This number should be the same as or close to the maximum number of threads that is selected on the Symantec AntiVirus Scan Engine. See "Selecting the maximum number of threads available for scanning" on page 6.
Connection timeout (seconds)	180 The default setting of 70 seconds does not allow sufficient time for the Symantec AntiVirus Scan Engine to decompose and scan all of the embedded files in larger archive and container file formats. This setting should match the maximum extract time that is selected on the Symantec AntiVirus Scan Engine for container file processing limits. The default setting on the scan engine is 180 seconds.
Patience page	Enabled Enabling the patience page prevents a connection time-out from occurring while the requesting Web browser waits for the Symantec AntiVirus Scan Engine to decompose and scan unusually large files.
Method supported	For incoming HTTP traffic, use: Response modification For outgoing HTTP traffic (POST transactions), use: Request modification
Preview size	4 bytes **Note:** To ensure proper functionality for virus scanning, you must set the preview size to 4 bytes. Virus scanning will not occur when any other value is used for this setting.

Creating an ICAP cluster

If you are using multiple scan engines to handle larger scan volumes, you must create a separate ICAP service cluster for both incoming and outgoing traffic and add the appropriate ICAP services into the cluster configuration. For incoming traffic, the cluster must contain the defined scan engine ICAP services that support the Response modification method. For outgoing traffic (to provide scanning for POST transactions), the cluster must contain the defined scan engine ICAP services that support the Request modification method. The Blue Coat Security appliance will not let you to cluster ICAP services with different methods together.

This lets you select the cluster as the virus scanner (rather than an individual scan engine) when you set up your Web Content and Web Access Policies so that load balancing is handled automatically through the cluster configuration. You can create the ICAP service cluster using the Blue Coat Security appliance Management Console or the Blue Coat command-line mode.

For more information, see the Blue Coat Security appliance documentation.

Creating Web Content and Web Access Policies for virus scanning

You must create a Web Content Policy on the Blue Coat Security client for virus scanning and configure the scan engine ICAP service or cluster as the virus scanner for the policy.

For more information, see the Blue Coat Security appliance documentation.

You must specify the following when you configure the Web Content and Web Access Policies for virus scanning:

- Which file types or MIME types to pass to the Symantec AntiVirus Scan Engine for virus scanning
  For maximum security, the recommended setting is to configure the Blue Coat Security client to pass all files to the Symantec AntiVirus Scan Engine for virus scanning, which lets the scan engine determine which files can contain viruses and scan accordingly.

  Note: Only the top-level file is examined by the Blue Coat Security client. Archive files might contain additional files that should be scanned for viruses. The list of file types to be sent to the Symantec AntiVirus Scan Engine for scanning should include archive and container file types.

- The ICAP service or cluster that will perform the scanning
  Select the ICAP service or the ICAP cluster that you created for the Symantec AntiVirus Scan Engine.
- The manner in which files are handled when the scan engine is unavailable for any reason or an error is generated in scanning a file
  For maximum security, the recommended setting is Deny the request. (Depending on the version of Blue Coat Security that you are running, this setting might be called Fail Closed.) Selecting Deny the request (Fail Closed) denies access to a file when the file has not been scanned, whereas selecting Bypass ICAP service (Fail Open) lets unscanned files pass through when the scan engine is unavailable for any reason or an error is generated during a scan.

Known issues with the Blue Coat Security appliance

The Blue Coat Security appliance might occasionally time out while waiting for a reply from the Symantec AntiVirus Scan Engine when extremely large or complex files are being scanned. If the Patience Page setting is enabled on the Blue Coat Security appliance and a scan request times out, the user receives no notification that a time-out occurred, and the Patience Page refreshes indefinitely. If the Patience Page setting is not enabled and a scan request times out, the Blue Coat Security appliance sends an ICAP communication error to the browser.

The likelihood of a time-out can be decreased by increasing the connection time-out setting to the recommended value (180 seconds) on the Blue Coat Security appliance.